

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (previously presented) A method for maintaining a security profile throughout nested service invocations on a distributed, component-based system, comprising the steps of:

- (a) providing interconnections between distributed components each having nested service invocations;
- (b) identifying a user;
- (c) associating the user with roles;
- (d) creating a user context instance upon successful identification of the user, wherein the user context instance includes information about the user including the roles and a unique user identifier;
- (e) receiving a request from the user to invoke a first service on a first component, wherein the first component invokes a second service of a second component such that the user context instance is passed as a parameter from the first component to the second component, and wherein completion of the second service is necessary to complete the first service;
- (f) querying the user context instance for the unique user identifier;
- (g) comparing the unique user identifier in the user context instance with an access control list for verifying that the user has access to the first component; and
- (h) comparing the unique user identifier in the user context instance with an access control list for verifying that the user has access to the second service of the second component.

2. (original) A method as recited in claim 1, further comprising the step of logging all user interactions.

3. (previously presented) A method as recited in claim 1, further comprising the step of modifying a user interface to provide access to actions that can be performed by the user based on the unique user identifier and the roles associated with the user.

4. (canceled)

C44/6. (currently amended) A method as recited in claim [[4]] 1, wherein the first service invoked associates any objects created, updated, or deleted as a result of the invocation of the first service with the user context instance.

C55/6. (original) A method as recited in claim 1, wherein the user context instance encapsulates security certificates of the user.

6/6. (previously presented) A computer program embodied on a computer readable medium for maintaining a security profile throughout nested service invocations on a distributed, component-based system, comprising:

- (a) a code segment that provides interconnections between distributed components each having nested service invocations;
- (b) a code segment that identifies a user;
- (c) a code segment that associates the user with roles;
- (d) a code segment that creates a user context instance upon successful identification of the user, wherein the user context instance includes information about the user including the roles and a unique user identifier;
- C6 (e) a code segment that receives a request from the user to invoke a first service on a first component, wherein the first component invokes a second service of a second component such that the user context instance is passed as a parameter from the first component to the second component, and wherein completion of the second service is necessary to complete the first service;
- (f) a code segment that queries the user context instance for the unique user identifier;
- (g) a code segment that compares the unique user identifier in the user context instance with an access control list for verifying that the user has access to the first component; and
- (h) a code segment that compares the unique user identifier in the user context instance with an access control list for verifying that the user has access to the second service of the second component.

C7 8. (original) A computer program as recited in claim 7, further comprising a code segment that logs all user interactions.

C8 9. (previously presented) A computer program as recited in claim 7, further comprising a code segment that modifies a user interface to provide access to actions that can be performed by the user based on the unique user identifier and the roles associated with the user.

C10 10. (canceled)

C9 11. (currently amended) A computer program as recited in claim 11, wherein the first service invoked associates any objects created, updated, or deleted as a result of the invocation of the first service with the user context instance.

C10 12. (original) A computer program as recited in claim 12, wherein the user context instance encapsulates security certificates of the user.

C11 13. (previously presented) A system for maintaining a security profile throughout nested service invocations on a distributed, component-based system, comprising:

- (a) logic that provides interconnections between distributed components each having nested service invocations;
- (b) logic that identifies a user;
- (c) logic that associates the user with roles;
- (d) logic that creates a user context instance upon successful identification of the user, wherein the user context instance includes information about the user including the roles and a unique user identifier;
- (e) logic that receives a request from the user to invoke a first service on a first component, wherein the first component invokes a second service of a second component such that the user context instance is passed as a parameter from the first component to the second component, and wherein completion of the second service is necessary to complete the first service;
- (f) logic that queries the user context instance for the unique user identifier;

- C11
- (g) logic that compares the unique user identifier in the user context instance with an access control list for verifying that the user has access to the first component; and
 - (h) logic that compares the unique user identifier in the user context instance with an access control list for verifying that the user has access to the second service of the second component.
-

C12 13/ 14. (original) A system as recited in claim 13, further comprising logic that logs all user interactions.

C13 13/ 15. (previously presented) A system as recited in claim 13, further comprising logic that modifies a user interface to provide access to actions that can be performed by the user based on the unique user identifier and the roles associated with the user.

E 16. (canceled)

C14 14/ 17. (currently amended) A system as recited in claim [[16]] 13, wherein the first service invoked associates any objects created, updated, or deleted as a result of the invocation of the first service with the user context instance.

C15 15/ 18. (original) A system as recited in claim 13, wherein the user context instance encapsulates security certificates of the user.
